



# CloudShield™

**High Performance Fault Tolerant Networking**

Dynamic Quarantine Industry Day Workshop

DARPA

March 4, 2003

Presented By:

CloudShield Technologies

Approved for public release; distribution is unlimited. #42451



# Worm Activity

- **Possible worm activity may be flagged by traffic analysis**  
*e.g. Dartmouth ICMP reject research*
- **Capture and redirection of ICMP reject packets to central analysis system may provide clue as to worm propagation method**
- **Suspect traffic can then be rate limited or blocked completely**
- **Once completely understood, complete packet inspection required to block worm packets**

*Automated Systems required with ever increasing propagation speeds.*



# Defense in Depth ... and Breadth

- **Extend Visibility into Core (fiber) Network**
- **Gain Full Visibility into Packet Content (layer 7)**
- **Integrate Traffic Surveillance Analysis with Security Functions (such as ACL, IDS, firewall, etc)**
- **Centralized alarm reporting & analysis**

*Effective **High Performance, Fault Tolerant Networking** requires **Full** Packet Inspection, logging and filtering on high speed (core) links*



# Key HPFTN Requirements in the Core

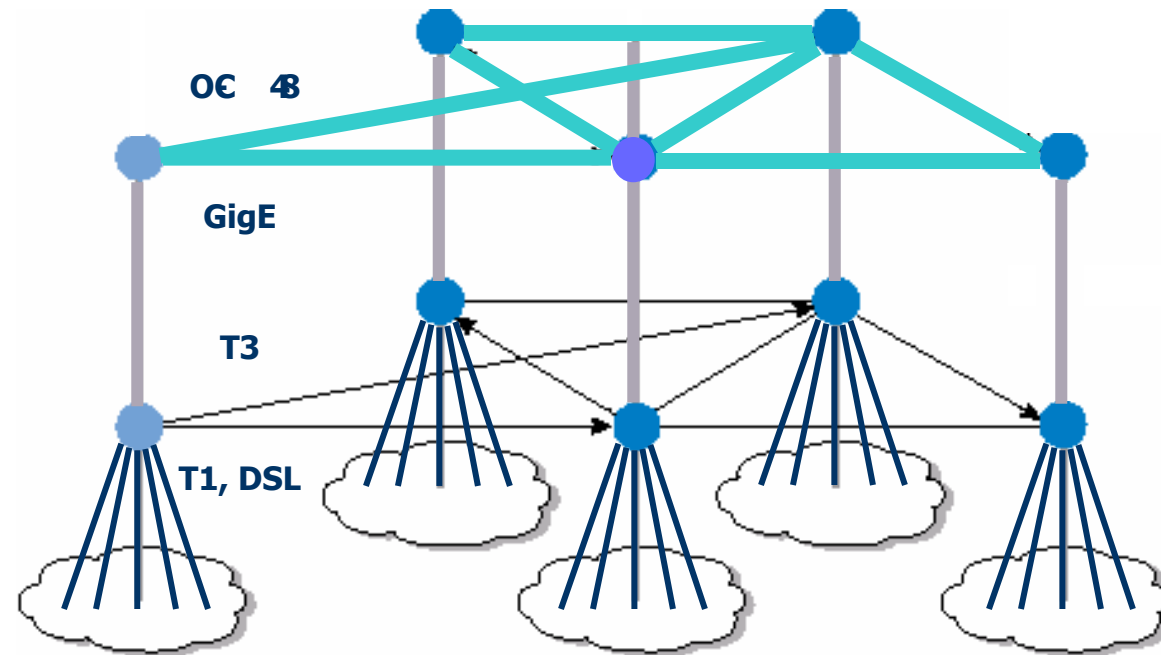
## **Performance**

The ability to perform 100%, full packet processing functions at optical speeds (OC-48c) without degrading network performance.

## **Flexibility**

The ability to run multiple application functions concurrently and rapidly re-program the platform to run different applications, whether platform-native, customer legacy, or rapidly designed, custom-built applications by the user.

# Approach to HPFTN Operations



## Tier 1 - Core

- Traffic Surveillance
- ACLs
- DDoS Filtering
- DNS Protection

## Tier 2 - Access

- Stateful Firewall
- Intrusion Detection
- Session Encryption

## Tier 3 - Enterprise

- Password Authentication
- Virus Protection

*HPFTN - Defense in Depth - Core, Access, and Enterprise*

# HPFTN Core Network Assurance Engine



Data Stream



OC-48  
or GigE

## Traffic Classification

- Layer 2 Header
- Layer 3 Header
- Layer 4 Header

## Treatment

- Forward/Drop
- Rate Limit
- Modify
- Duplicate
- Log
- Count
- Etc.

## Extended Inspection

- Application Headers
- Application Data
  - String Search
- Connection State
- Etc.

## Treatment

- Forward/Drop
- Rate Limit
- Modify
- Duplicate
- Log
- Count
- Etc.

**When populated with customer data and rule sets, this engine enables:**

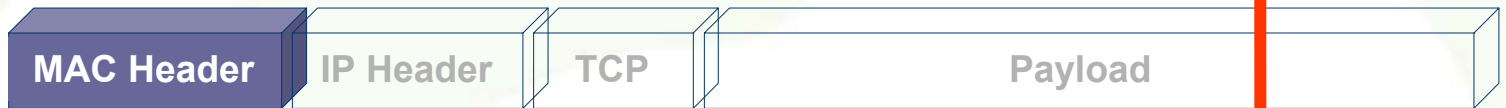
- Traffic Surveillance
- Access Control Lists
- DDoS/Virus Blocking
- Stateful Packet Inspection
- Attack Recognition
- DNS Protection
- Statistics
- Reporting
- Customer Defined Apps...



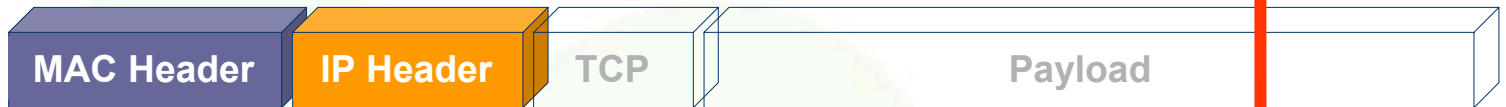
# HPFTN Content-Aware Packet Inspection



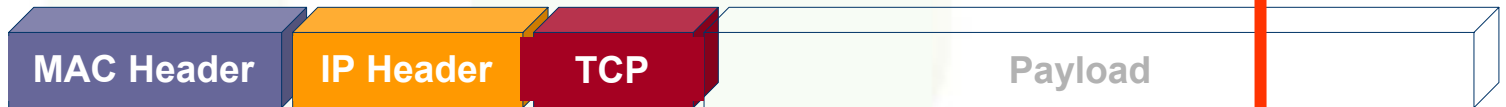
Switch



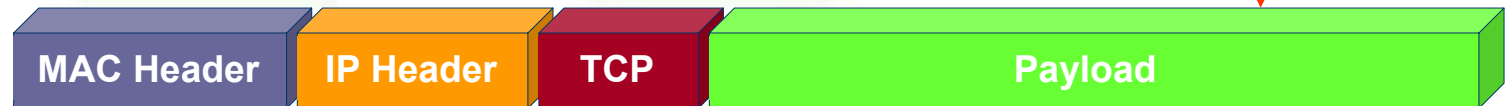
Router



Firewall



FTNP



14 Bytes

20 Bytes

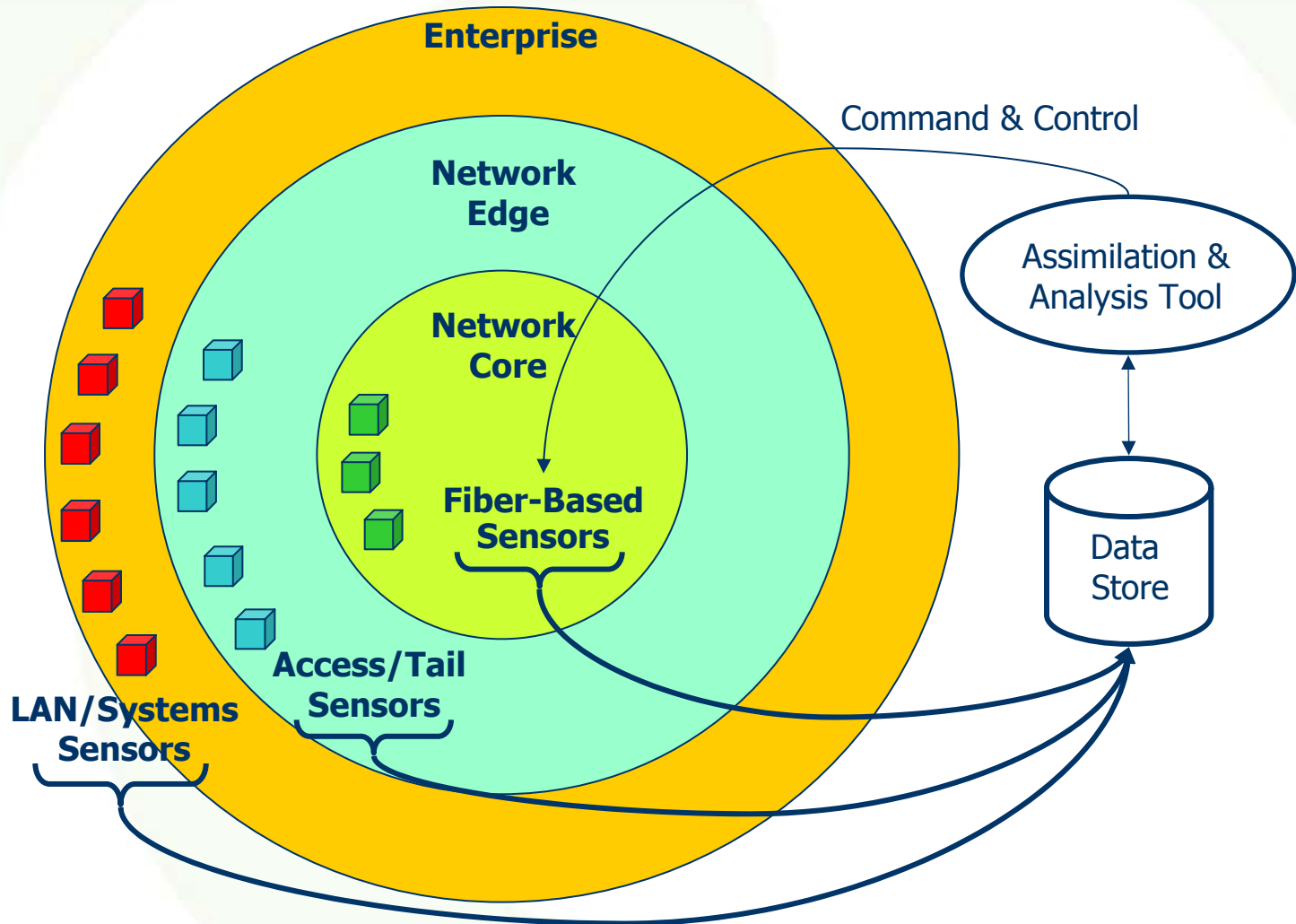
20 Bytes

48 - 8,192 Bytes

Variable

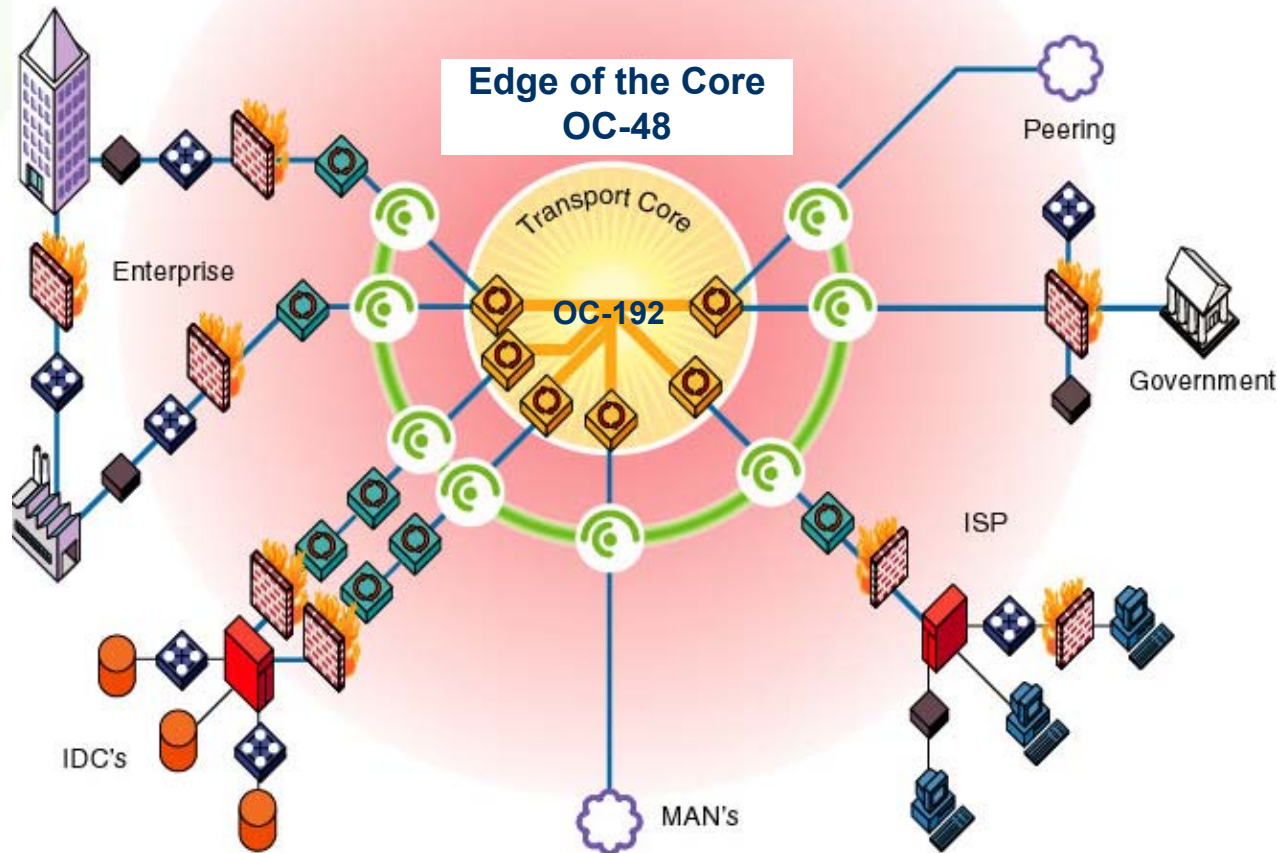
Code Red / NIMDA,  
Macro Viruses, etc.

# FTN Management - Sensor Data Fusion



*FTN requires data from ALL sensors to be correlated & analyzed*

# Core-Based HPFTN Sensor Paradigm



*Core-Based HPFTN Enables Early Warning and Response Capabilities for Network Operators & Users*



# Why a HPFTN Platform in the Core

- **Extend “Intelligent Sensor” concept to fiber networks**

- Build secure, high-speed networks that are resilient to attack
- Sit actively or passively on OC48 or GigE fiber links
- Inspect all packets & collect statistics about the different traffic flows (*service type, source ID, destination ID, packet length, arrival time, etc*)
- Rapid-prototype & deploy new rules or applications (*threat agility*)

- **Perform Content-Aware, Realtime Traffic Surveillance**

- Continuously monitor “host” network (*passive or active probe, etc*)
- Provide realtime traffic statistics to central data warehouse for analysis
- Protocol level, policy enforcement (*e.g., RFC compliance*)
- Deploy high-performance FTN functionality closer to the core
  - ACL, IPS, firewall, DDoS, Worm type detection & response

- **Critical Infrastructure Protection**

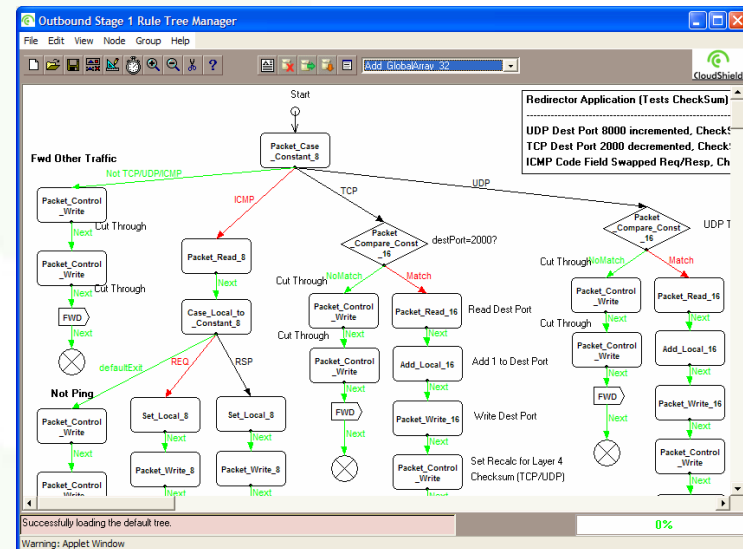
- Monitor the health and status of the link and provides information to Enterprise NMS system
- Secure routers, DACS, switches and infrastructure from cyber-attack

# Overview of the CloudShield System



## A High Performance Platform for HPFTN Applications

- General Purpose packet processing platform
- First platform Capable of **OC-48 Performance** (GigE also Available)
- Capable of running many types of **Applications**
- **Full Layer 2-7 Content Inspection** without Performance Degradation
- Installation with **NO** Network Reconfiguration
- **RAVE™** enables rapid prototyping of new apps
- 4GL-language for user programmability





# Suggested area of research

- Integration of network core based packet inspection platforms with automated analysis tools to form complete worm detection, identification, and blocking system.
- Simulations/demonstrations on suitable testbed networks; e.g. DREN
- Automated interaction between core based sensor platforms to foster faster network responses to threatening activity.

# Questions?



Peder Jungck,  
Founder & CTO

CloudShield Technologies, Inc.  
212 Gibraltar Dr.  
Sunnyvale, CA 94089  
408.331.6640

[peder@cloudshield.com](mailto:peder@cloudshield.com)

[www.cloudshield.com](http://www.cloudshield.com)



CloudShield's  
FTN Platform